ds dnevi slovenske informatike 20 let

"Dvajset let pozneje"

Kongresni center Grand hotel Bernardin
Portorož | Slovenija | 15. - 17. april 2013

20. konferenca
Dnevi slovenske informatike

Informacijska varnost - obravnava incidentov

mag. Damijan Marinšek, MNZJU

Gorazd Božič, SI-CERT

17. 04. 2013

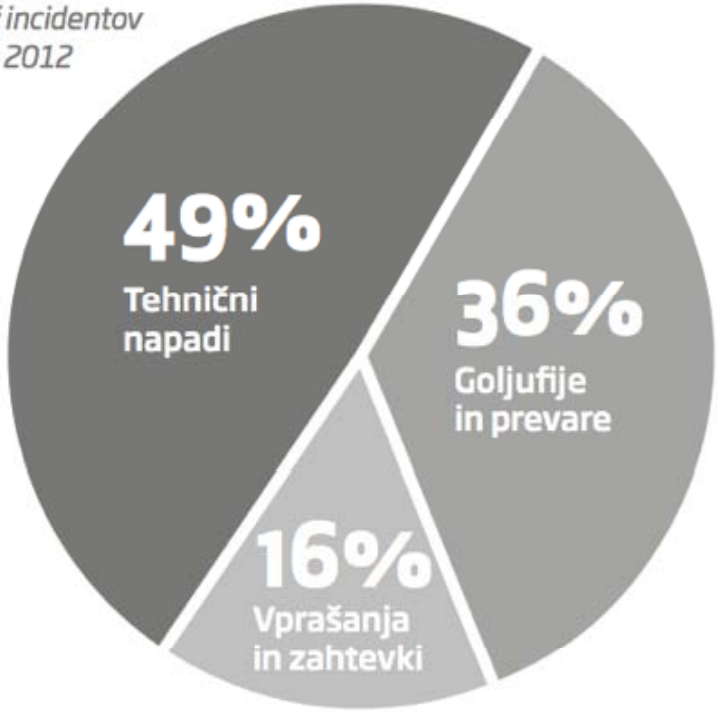
slovensko društvo informatika

SI-CERT

- nacionalni odzivni center za omrežne incidente
- ustanovljen 1995, lociran v Arnesu
- akreditiran v programu Trusted Introducer
- član FIRST - Forum of Incident Response and Security Teams
- od 2010 tudi CERT za sisteme v javni upravi
  - sklep Vlade RS 38600-3/2009/21 z dne 8.4.2010


1300
976
650
326
0
2008
2009
2010
2011
2012
43%
59%
64%

Delež incidentov v letu 2012



Obravnave incidentov v letu 2012

2727 prijav na SI-CERT

1250 odprtih primerov

946 preiskav

4165 poslanih elektronskih sporočil

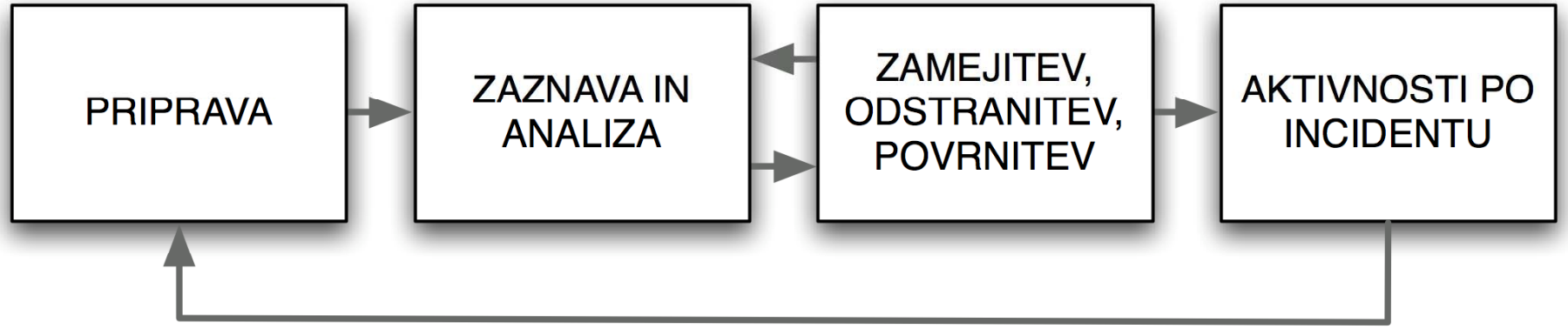
Najpogostejši incidenti v letu 2012

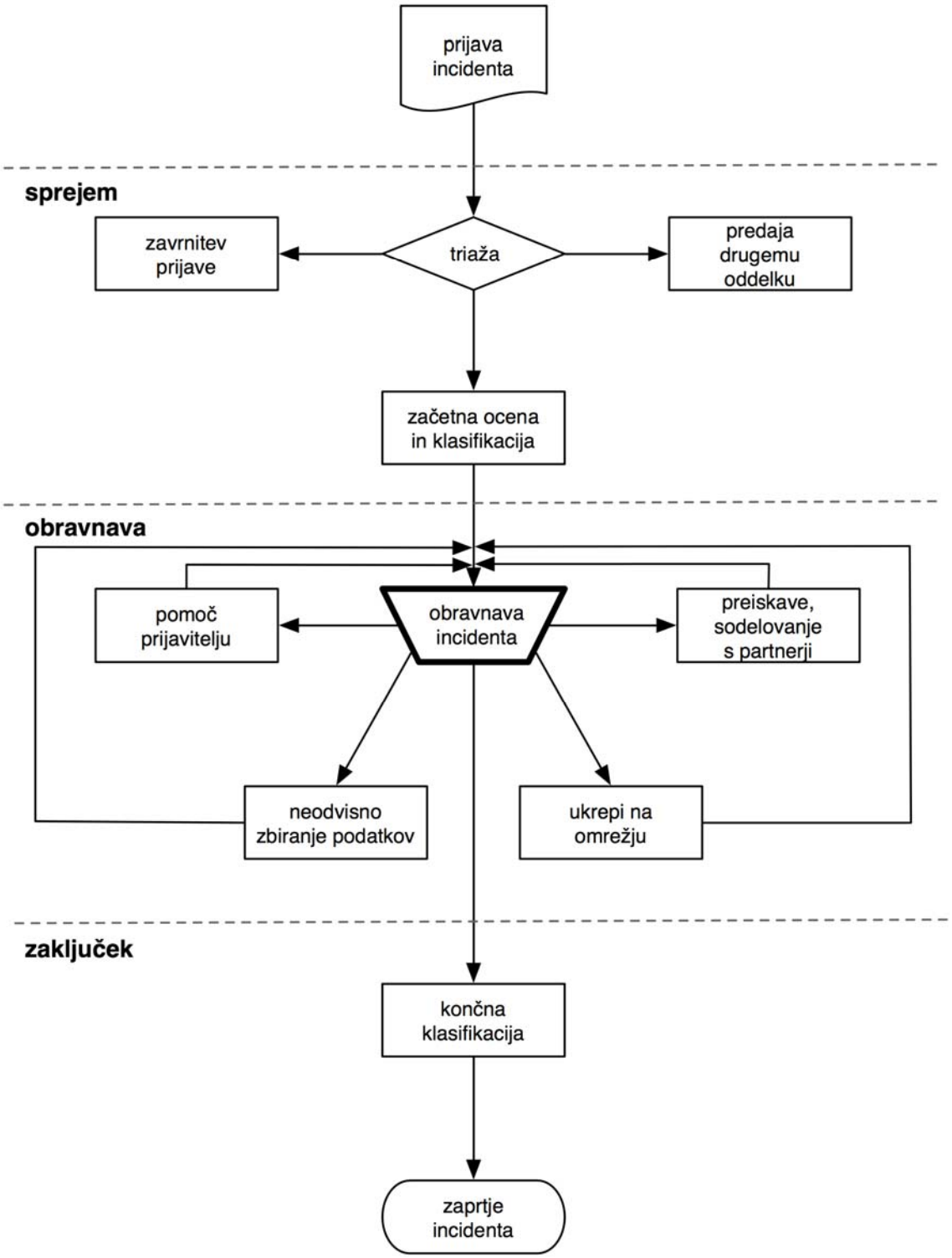
258 preiskav škodljive kode

125 primerov razobličenj, v njih obvestili 428 skrbnikov strežnikov in nosilcev domen

100 % porast phishing napadov in goljufij

Obravnava incidenta




prijava incidenta
sprejem
zavrnitev prijave
triaža
predaja drugemu oddelku
začetna ocena in klasifikacija
obravnava
pomoč prijavitelju
obravnava incidenta
preiskave, sodelovanje s partnerji
neodvisno zbiranje podatkov
ukrepi na omrežju
zaključek
končna klasifikacija
zaprtje incidenta

Škodljiva koda

Dear,

Please find enclosed herewith document regarding the latest situation in Kosovo.

Should you need further information do not hesitate to contact us!

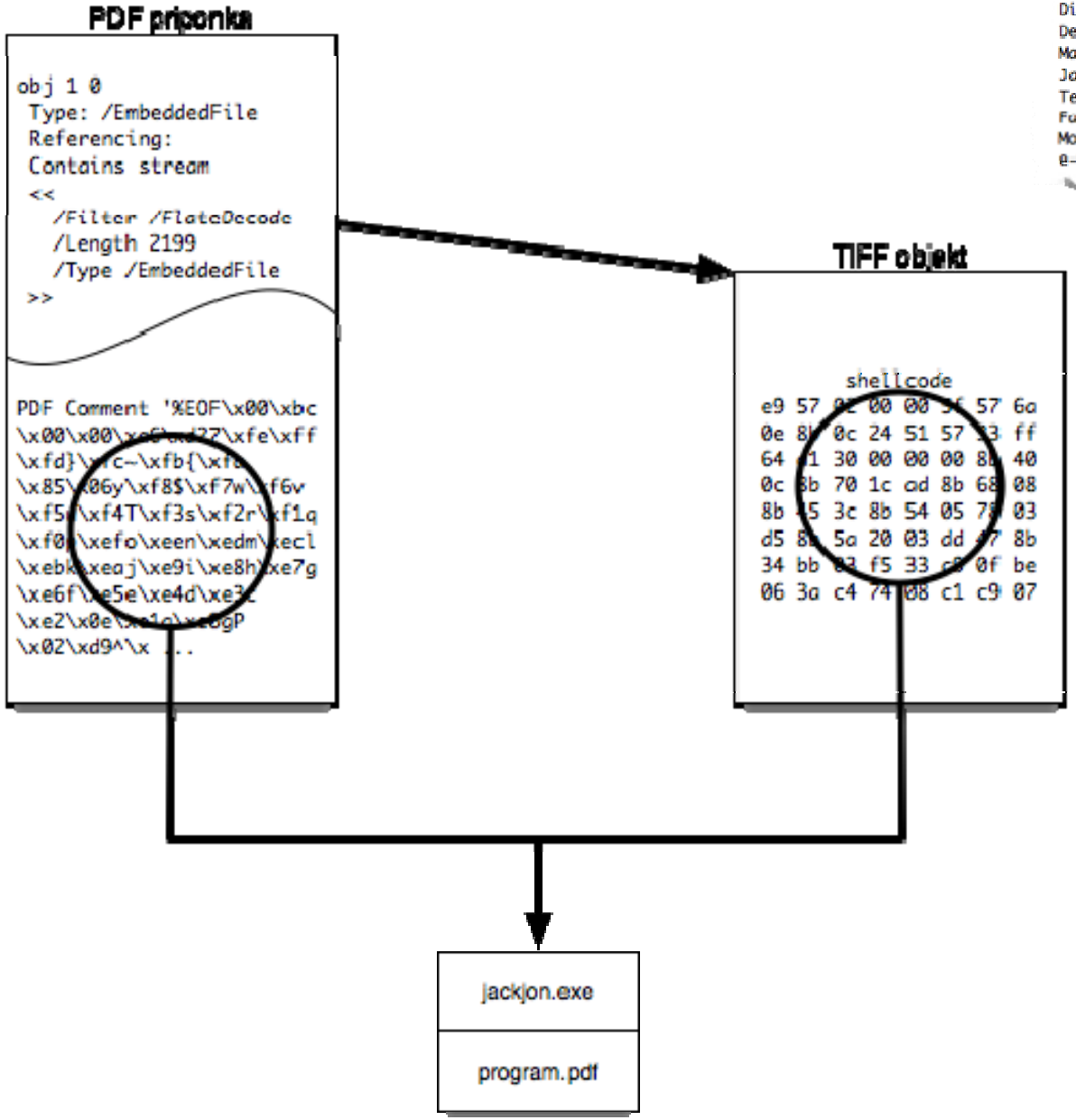
Best regards,
Ria Uki Suharsi (Ms)
Directorate of Dialogue Partners and Inter-Regional Cooperation
Directorate General of ASEAN Cooperation
Department of Foreign Affairs
Main Building, 8th Floor
Jakarta
Tel. + 62 21 381 2933
Fax: +62 21 385 8042
Mobile: +62 815 749 351 89
e-mail: ria.suharsi@gmail.com

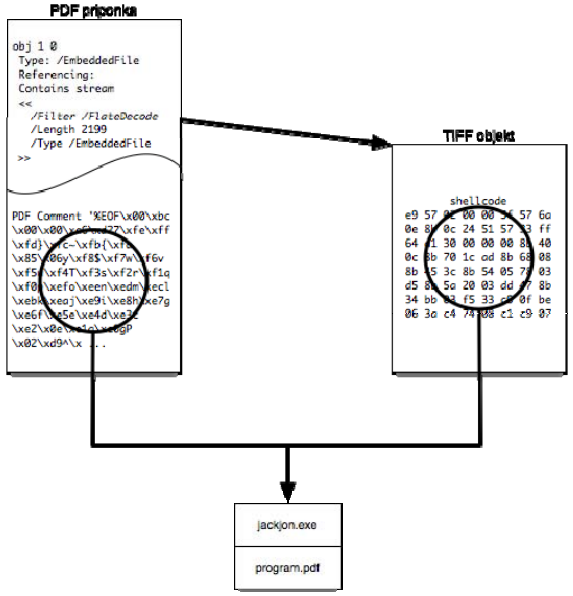
Dear,

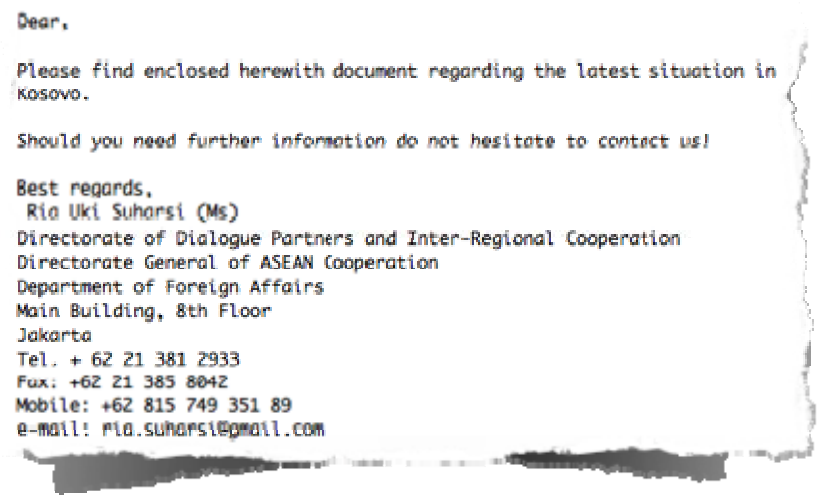
Please find enclosed herewith document regarding the latest situation in Kosovo.

Should you need further information do not hesitate to contact us!

Best regards,
Rio Uki Suharsi (Ms)
Directorate of Dialogue Partners and Inter-Regional Cooperation
Directorate General of ASEAN Cooperation
Department of Foreign Affairs
Main Building, 8th Floor
Jakarta
Tel. + 62 21 381 2933
Fax: +62 21 385 8042
Mobile: +62 815 749 351 89
e-mail: rio.suharsi@gmail.com







"MiniEvil by FaceOl"

2615	2430.506976	194.249	193.2.1.66	DNS	Standard query A webmail.antivirtusbar.com
2616	2430.519631	193.170	194.249.241.1(	TCP	[TCP segment of a reassembled PDU]
2617	2430.519869	194.249	193.170.140.7(	TCP	netarx > http [ACK] Seq=278 Ack=1813708 Win=65535 Len=0
2618	2430.521029	193.2.1	194.249.241.1(	DNS	Standard query response A 123.120.121.35

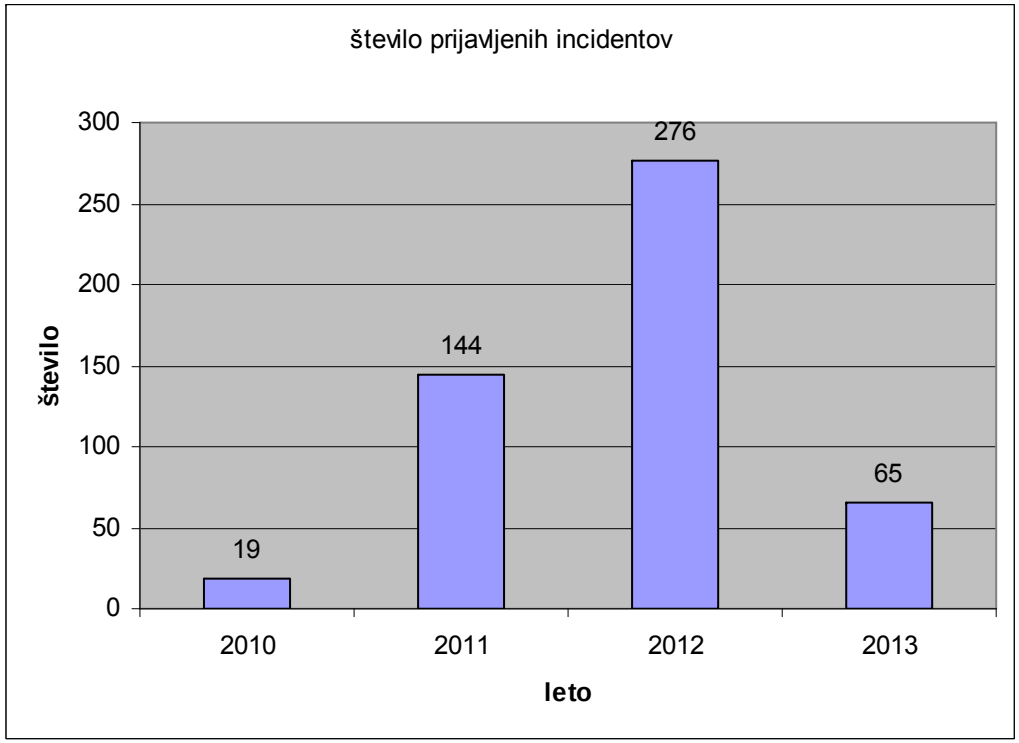
inetnum: 123.112.0.0 - 123.127.255.255
netname: UNICOM-BJ
descr: China Unicom Beijing province network
descr: China Unicom
country: CN

Ranljiva infrastruktura

- kritična infrastruktura
- SCADA
- toplotne postaje
- pametni števci
- *razširjena internet infrastruktura*

Kaj pa država?

Število incidentov od leta druge polovice leta 2010 po podpisu sporazuma in vzpostavitvi predala cert@gov.si.



Kaj pa država 2

- Vzpostavljen je mehanizem obveščanja. Obstajajo formalni in neformalni kontakti.
- Republika Slovenija je sodelovala na vaji Cyber Europe CE2012 skupaj z nekaj predstavniki ponudnikov storitev, dve banki in SICERT ter organi državne uprave.
- Izvedli smo tudi nacionalno vajo s tega področja.
- Manjka pa formalna ureditev in kadrovska popolnitev.

Hvala za vašo pozornost !

Vprašanja?

Pripombe?

Predlogi?